



UNITED STATES PATENT AND TRADEMARK OFFICE

A

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/801,725	03/09/2001	Tim King	1591.0050001/RES/RDL	5084
919	7590	11/03/2005	EXAMINER	
PITNEY BOWES INC. 35 WATERVIEW DRIVE P.O. BOX 3000 MSC 26-22 SHELTON, CT 06484-8000			DANG, KHANH	
			ART UNIT	PAPER NUMBER
			2111	
DATE MAILED: 11/03/2005				

Please find below and/or attached an Office communication concerning this application or proceeding.



UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

MAILED

NOV 03 2005

Technology Center 2100

**BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES**

Application Number: 09/801,725
Filing Date: March 09, 2001
Appellant(s): KING ET AL.

George M. Macdonald
For Appellant

SUPPLEMENTAL EXAMINER'S ANSWER

This is in response to the REPLY BRIEF filed 9/23/2005 appealing from the Examiner's

Answer mailed 7/25/2005.

In the Reply Brief, Appellants state that "Appellants do not concede that contemporaneous documentary support is available to show support of Official Notice, but it is arguable, that if such 'cited' documentary support is contemporaneous (if it itself is not available as prior art), it must at a minimum establish by a preponderance of evidence that the statement of official notice is unquestionably supportable as being well-known before the date required for the official notice to be effective as prior art in the case." See page 3 of the Reply Brief.

In response to Appellants' argument, the Infospace Search Engine for mapping a physical address to an email address is notoriously old and well-known, and is well before the filing date of the instant application. To further support the fact that Infospace Search Engine is old and well-known, the following documents are further provided:

1) The Ultimate Email Directory, 1997, features Infospace, among other similar Email Search Engines, to provide mapping a physical address to an email address. A copy of "The Ultimate Email Directory" is attached to this Supplemental Examiner's Answer. A screenshot is provided below:

Art Unit: 2111

The Ultimate Email Directory - Microsoft Internet Explorer provided by USPTO

Back Forward Stop Refresh Home Search Favorites History Mail Print Edit Discuss Windo...

Links USPTO Intranet Homepage Customize Links Free Hotmail Windows Windows Media

Address http://web.archive.org/web/19980117035142/http://www.theultimates.com/email/ Go

Google Search Check AutoLink AutoFill Options

File Edit View Favorites Tools Help

THE ULTIMATE EMAIL DIRECTORY

Not a robot

[Home | White Pages | Yellow Pages | Email Directory | Trip Planner | Compliments and Awards]

Four11: Last: <input type="text"/> First: <input type="text"/> City: <input type="text"/> State: <input type="text"/> Country: <input type="text"/> Organization: <input type="text"/> Domain: <input type="text"/> <input type="button" value="Search"/>	WhoWhere: Name: <input type="text"/> Domain: <input type="text"/> <input type="button" value="Search"/>	IAF: Last: <input type="text"/> First: <input type="text"/> Organization: <input type="text"/> Domain: <input type="text"/> <input type="button" value="Search"/> Reverse (IAF): <input type="text"/> Email: <input type="text"/> <input type="button" value="Search"/>	InfoSpace: Last: <input type="text"/> First: <input type="text"/> City: <input type="text"/> State: <input type="text"/> Country: <input type="text"/> <input type="button" value="Search"/>	Bigfoot: Name: <input type="text"/> <input type="button" value="Search"/> <input type="button" value="Reset All"/>	ESP: Name: <input type="text"/> <input type="button" value="Search"/> <input type="button" value="Reset All"/>
--	---	--	---	--	--

Newcomers:

Welcome to the Ultimate Email Directory!

Have you ever lost an important email address?
 We all have. Trying to find it is frustrating. There are six different email directories on the Internet, all with different data sources and different degrees of accuracy. The Ultimate Email Directory is a common interface to all six.

This site is designed to be fast and simple. Just type your search criteria into the first search engine (Four11). Type in all the items you know. The items applicable to the other engines will be automatically copied to the other forms by a Javascript applet. Then hit Search on the first search engine you want to query. A new browser window will open with the search results. Then switch back to the original window and hit submit on the next one. You can search as many as you want until you are satisfied with the results.

Questions?
 Read the [FAQ](#). If you don't find an answer, email me.

Email Directory Administrators: Don't want your engine used on this page? Or do you want more credit for it? I'll be happy to change my page if you want me to.

page made and administered by [Scott Martin](#)

This page has been accessed 119425 times since May 31, 1997.

Legal Gibberish with Translations

The Ultimates are ©1997 by Scott Martin.

Start 6 M. 12:17 Win... 3 R. My ... eDA... 2 M. 4 E. 3 M. 2:55 PM

In reference to claims 5 and 13, According to 37 CFR 1.196(b), if the Board determines that claims 5 and 13 are sufficiently broad enough that a 35 USC 102 may have been applied instead of the Examiner's 35 USC 103 rejection, the Examiner respectfully requests that the Board, in the decision, to include a statement that constitutes a new ground of rejection of claims 5 and 13. The server, maintained by Infospace, allows a user to specify a physical address of a recipient in the address box, and performing mapping a physical address to an email address, or in other words, searching a recipient's email address using a recipient's physical address in a database comprising the recipient's physical address and email address. The user may then uses the obtained email address to send or route email to the recipient.

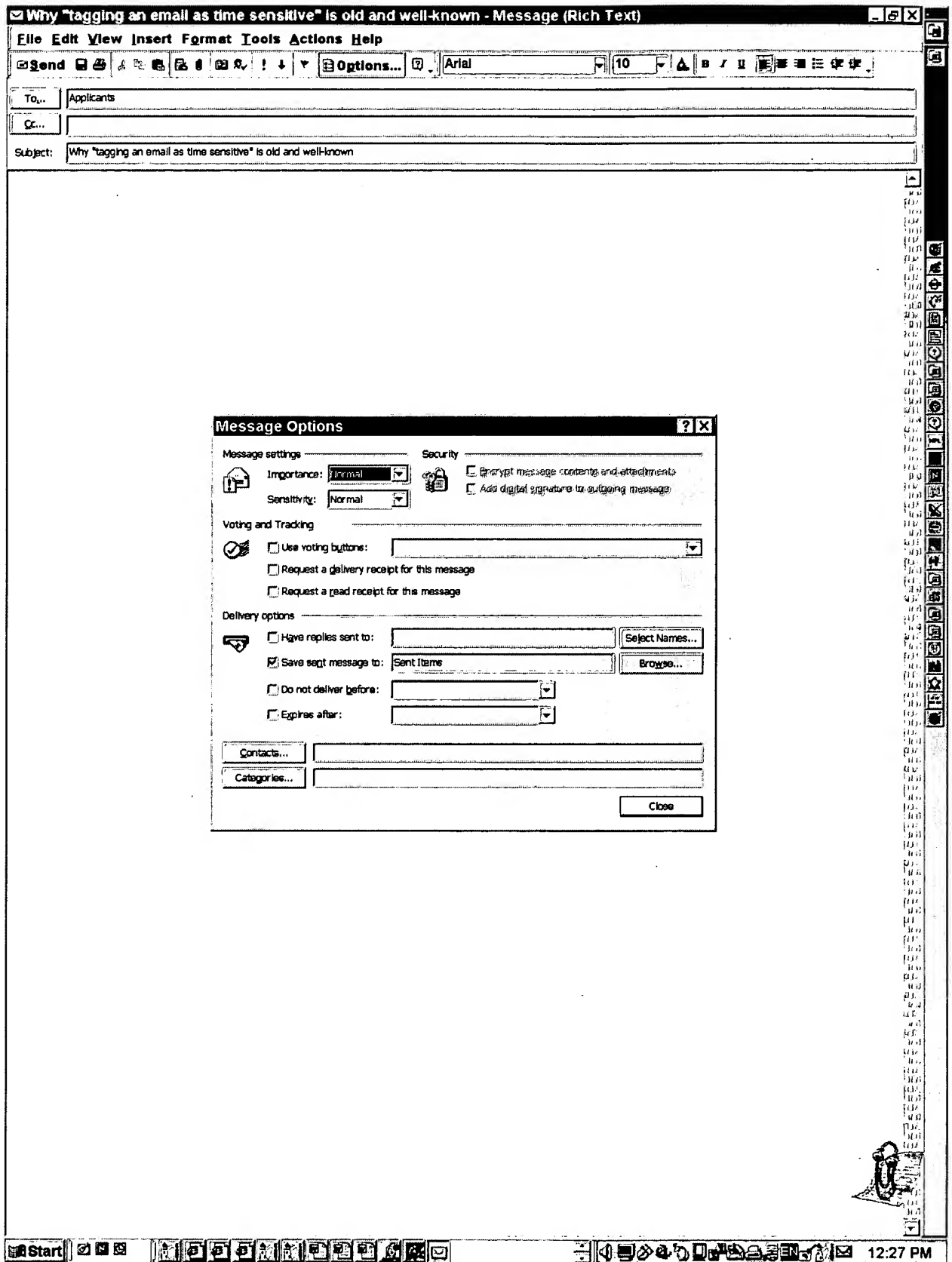
Appellants further argue that "it is not clear whether such alleged documentary support is now cited as prior art (for the first time) without sufficient bases. See Examiner's Answer at page 3. Such references were never cited on a PTO-892 and Appellants do not concede that they are available. Similarly, patents listed as prior art are not available against the present application and any application of them is respectfully traversed. For example, the earliest priority dates of Baird III et al. (6,732,278) and Creswell, et al. (6,775,690) are both after the effective filing date of the present case and not available.

In response to Appellants' argument, all US Patent Documents, cited in the Examiner's Answer, have already been cited in PTO-892 in previous Office Action. Copies (screenshots) of web sites, cited as evidences of well-known facts, are directly provided in the form of screenshots (such as the screenshot of "The Ultimate Email Directory" shown above) in every previous Office Actions.

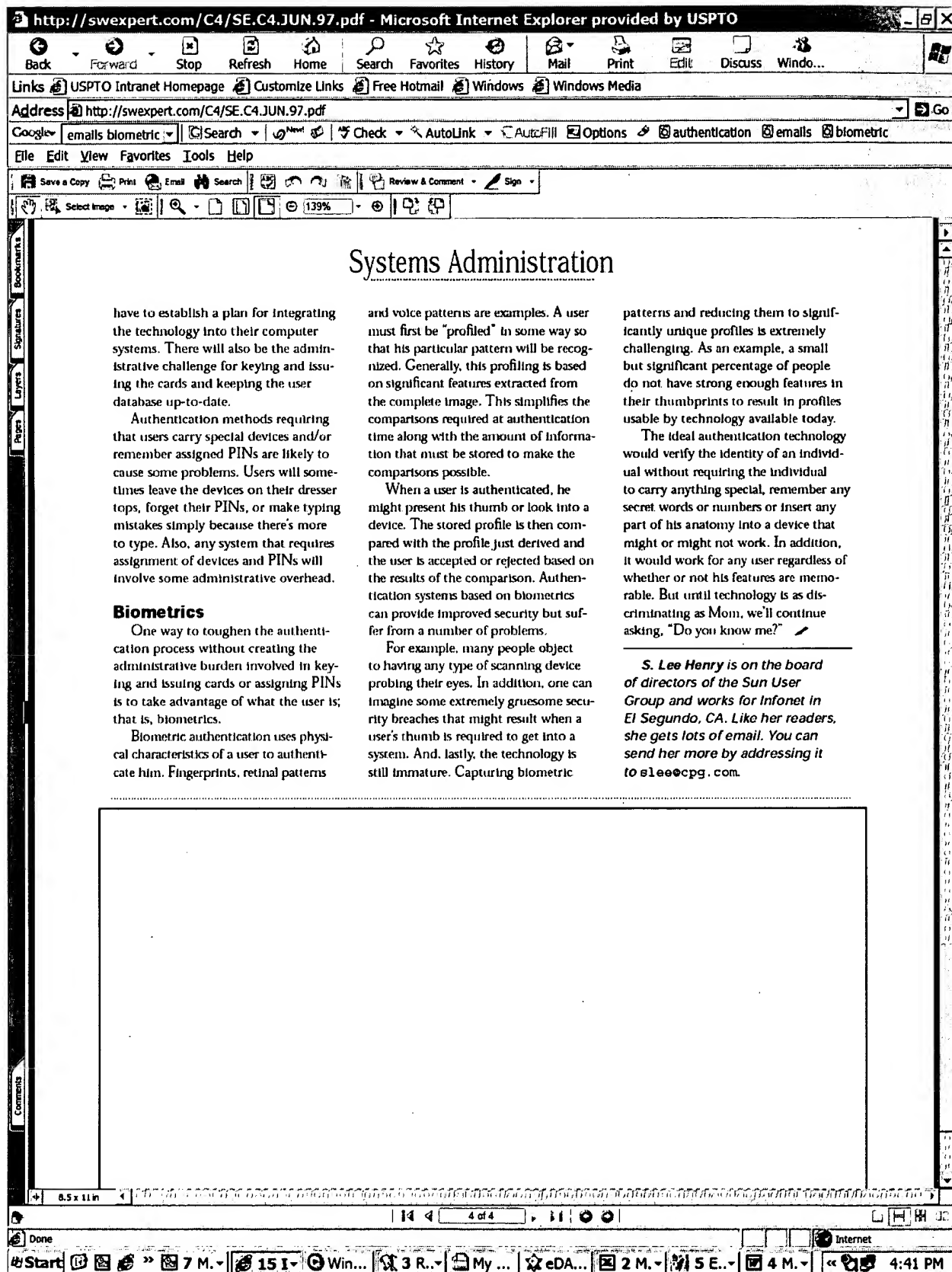
In reference to Baird III et al. (6,732,278) and Creswell, et al. (6,775,690), The Examiner agrees with Appellants that the earliest priority dates of Baird III et al. (6,732,278) and Creswell, et al. (6,775,690) are both after the effective filing date of the present case. It is acknowledged that the provisional filing date of the present application has been overlooked. It is also noted that the priority dates of Baird III et al. (6,732,278) and Creswell, et al. (6,775,690) have never been challenged until this Reply Brief from Appellants.

In rejecting claim 12 under 103 rejection, the Examiner stated that "tagging selected emails as time sensitive" is old and well-known as evidenced by Creswell et al. (6,775,690) or Microsoft Outlook. The Examiner still maintains that "tagging selected emails as time sensitive" is old and well-known as evidenced by at least Microsoft Outlook. The following is a screenshot showing "Message Options" in Microsoft Outlook. One can set the "importance" of an email by checking either Normal, High, or Low. It is clear that emails with High Importance level will require attention in a more timely fashion than those with Low Importance level. In another word, the emails sent using Microsoft Outlook can be tagged as time sensitive.

Art Unit: 2111



In rejecting claim 15 under 103 rejection, the Examiner stated that using biometric identification to allow users access to an email server is old and well-known as evidenced by Baird III et al. (6,732,278). The Examiner still maintains that using biometric authentication is old and well-known as evidenced by "Authentication Basics" (1977). A copy of "Authentication Basics" is attached to this Supplemental Examiner's Answer. An example screenshot of the document is provided below:



In page 4 of Appellants' reply brief, Appellants argue that the statement: mapping a physical address to an email address "is presented for the first time in the Examiner's Answer and not in the Final Rejection at page 4."

In response to Appellants' argument, in page 4 of the Final Rejection, the Examiner clearly stated that "searching a particular predetermined information using a key word or phrase in a data base is old and well-known." In page 12 of the Final Rejection, the Examiner further stated that "it is clear that searching a data base using keywords includes searching any kind of database including email address database, for example. It is also clear that using keywords includes using any desired keywords including keywords specifying a physical address. As a matter of fact, using a search engine to find an email address using a physical address is notoriously old and well-known." In page 13, a screenshot of Infospace email directory was provided as documentary evidence.

Infospace discloses searching for a predetermined information (email address) using a key words (physical address) in a database. It is clear that searching a person's email address using a person's physical address in a database comprising the person's physical address and email address is "mapping a physical address to an email address."

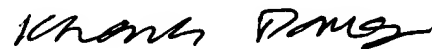
The Examiner also maintains that Infospace Search Engine for mapping a physical address to an email address is notoriously old and well-known, and is well

Art Unit: 2111

before the filing date of the instant application. The "Ultimate Email Directory" featuring Infospace, among other similar Email Search Engines, at least exists in 1997, to provide mapping a physical address to an email address.

For the above reasons and the reasons set forth in the Examiner's Answer, it is believed that the rejections should be sustained.

Respectfully submitted,



Khanh Dang
Primary Examiner

Khanh Dang
Primary Examiner

Systems Administration

by S. Lee Henry



Authentication Basics

Several years ago, American Express aired a series of TV commercials featuring folks with household names but not household faces. "Do you know me?" they asked, before their name typed itself across the screen. Though the concept of using our credit cards to prove who we are might seem a little error-prone to those of us who have at some point lost ours, the process of identifying ourselves to our computer systems is considerably more error-prone. Passwords, the primary method for controlling access to computer systems, are subject to serious abuse.

At the same time, technology exists to improve the situation significantly. Advances in authentication services, designed to augment or replace passwords, help ensure that authorized users can uniquely identify themselves to their computer systems while impostors find virtual doors slammed in their virtual faces.

Of course, authentication is not new. Any process through which a user establishes the validity of his claimed identity

is authentication. The increased use of the word corresponds to the availability of increasingly sophisticated technology for making the authentication process more rigorous.

Though a related process, authentication is not the same as identification and, in fact, can almost be thought of as its opposite. While a person's identity is public, the way that he establishes this identity (i.e., authentication) often requires him to provide something that is secret—at least secret from everyone but him and the authenticator. Also, authentication is not only used during login but has other important uses. The three main types of authentication in a distributed computing system are as follows:

- User identity authentication – Verifying the identity of the user.
- Message origin authentication – Verifying that the sender of a message is, in fact, the sender claimed in the message.
- Message content authentication – Verifying that the message received is the message that was sent.

The latter two of these authentication types use some form of cryptology. These will be described in next month's column.

User Authentication

Whether a user is being authenticated by a login process or a security guard at the door, there are three basic means by which he establishes his identity. These involve his providing one or more of the following:

- Something that only he knows (a password, a PIN number or his mother's maiden name).
- Something that he possesses (a physical key or a "smartcard").
- Something physical that identifies him (biological features such as thumbprints or retinal scans).

Any of these, by itself, would be sufficient in certain situations, but, used in combination, these basic means of identification provide significantly stronger authentication than any single means alone. Access to restricted work environments (e.g., where classified information

Systems Administration

or dangerous substances are involved) commonly requires a combination of something one knows (e.g., a password or PIN) and something one has in one's possession (e.g., a picture ID).

Better Passwords

An established approach to improving the security of systems protected by passwords is to improve the passwords,

whether by insinuating rigorous checks into the change password process or by running crack-like programs after the fact to weed out passwords likely to be tried in brute force attacks.

Establishing a password that is easy to remember yet difficult to guess is a significant challenge. The basic problem is a matter of simple statistics. We all think pretty much the same

way—and there are a lot of us. It's likely that every clever idea regarding the construction of passwords has been considered numerous times before. Deliberate misspellings, combinations of words with and without attached digits, words in other languages, and look-alike character substitutions are popular "tricks" that the good guys as well as the bad guys have thought to try. Though better than single words and obvious personal associations, none of these tricks is foolproof (or should I say crackerproof?).

Clearly, the passwords that are hardest to guess are also the hardest to remember. Once we resort to writing down our passwords, we have moved the problem from our heads to our files. Where and how we keep track of these passwords and what access we and others have to them determines how good a solution we've created.

Another extremely important issue in password security is whether the same password is used on multiple systems. Even the cleverest password is subject to being snooped. If a password captured at one location provides access to accounts at numerous other locations, any other precautions we might take are meaningless.

The frequency with which passwords are changed might be defined by a security policy and/or implemented in the operating system itself. Periodic changing of passwords can limit the damage made possible through guessed, cracked or snooped passwords. On the other hand, if passwords are changed too often, the users themselves are likely to forget what they just set their passwords to and suffer periods in which they cannot log in.

Frequently changing passwords, in the extreme, may be expressed as single-use passwords. Generally, when single-use passwords are employed, we are dealing with what a person possesses rather than what he knows. Users are likely to have to mark off an entry in a list of passwords every time they log in, thereby keeping their logins synchronized with a process running on their systems. This type of scheme guards against compromised passwords being used by unauthorized individuals but

Systems Administration

creates something of an administrative burden as the lists must be generated, distributed and essentially managed by the users.

Better Than Better Passwords

To toughen the authentication process further, we can combine what a user knows with something he possesses. If

we hand our users something that they must have in their possession to log in and require them to have a password as well, we make it very difficult for anyone else to duplicate the login process. A variety of security add-ons are available that can serve this purpose—from memory cards and smartcards to handheld password generators, all of which combine something the user possesses

with something he knows.

Memory cards are frequently used in banking and physical access applications. Telephone calling cards, credit cards and ATM cards all serve, to some extent, to authenticate their users. In some cases, possession of the card alone (i.e., knowledge of the owner's name, the card number and the expiration date), is sufficient for both identification and authentication; this is clearly the key vulnerability where credit cards are concerned. Memory cards for system security applications that require the use of PINs along with the cards are much less vulnerable (unless, of course, the users keep their PIN with the card!). Generally, a lost or stolen card is a much less serious risk if a PIN is required for its use.

Smartcards are usually the size and shape of credit cards and contain integrated chips rather than magnetic strips like memory cards. Smartcards are, in fact, tiny computer systems. They contain a microprocessor and memory along with some means of providing input and output.

The smartcard can replace conventional password security with a PIN verified by the card and can be programmed to provide additional checks. It might, for example, limit the number of login attempts a user can make or challenge the user with questions. An important factor is that anyone who observes an authorized login should not be able to make off with the card and, thereby, repeat the process. It's also important that the cards be difficult to duplicate.

When a password generator is used for access to augment login security, an extra level of security is gained. Each user is given a device that is uniquely keyed and assigned to him; he cannot use someone else's device for access, and no one else can use his. The host system must have a corresponding process to generate a challenge/response pair for each login attempt, based on the entered user name. Because each challenge is different, no one observing a successful exchange can extract information that would enable them to log in.

Overall, this technology can be a useful addition to security, but users may find some inconvenience. Management, if they decide to use this approach, will

Systems Administration

have to establish a plan for integrating the technology into their computer systems. There will also be the administrative challenge for keying and issuing the cards and keeping the user database up-to-date.

Authentication methods requiring that users carry special devices and/or remember assigned PINs are likely to cause some problems. Users will sometimes leave the devices on their dresser tops, forget their PINs, or make typing mistakes simply because there's more to type. Also, any system that requires assignment of devices and PINs will involve some administrative overhead.

Biometrics

One way to toughen the authentication process without creating the administrative burden involved in keying and issuing cards or assigning PINs is to take advantage of what the user is; that is, biometrics.

Biometric authentication uses physical characteristics of a user to authenticate him. Fingerprints, retinal patterns

and voice patterns are examples. A user must first be "profiled" in some way so that his particular pattern will be recognized. Generally, this profiling is based on significant features extracted from the complete image. This simplifies the comparisons required at authentication time along with the amount of information that must be stored to make the comparisons possible.

When a user is authenticated, he might present his thumb or look into a device. The stored profile is then compared with the profile just derived and the user is accepted or rejected based on the results of the comparison. Authentication systems based on biometrics can provide improved security but suffer from a number of problems.

For example, many people object to having any type of scanning device probing their eyes. In addition, one can imagine some extremely gruesome security breaches that might result when a user's thumb is required to get into a system. And, lastly, the technology is still immature. Capturing biometric

patterns and reducing them to significantly unique profiles is extremely challenging. As an example, a small but significant percentage of people do not have strong enough features in their thumbprints to result in profiles usable by technology available today.

The ideal authentication technology would verify the identity of an individual without requiring the individual to carry anything special, remember any secret words or numbers or insert any part of his anatomy into a device that might or might not work. In addition, it would work for any user regardless of whether or not his features are memorable. But until technology is as discriminating as Mom, we'll continue asking, "Do you know me?"

S. Lee Henry is on the board of directors of the Sun User Group and works for Infonet in El Segundo, CA. Like her readers, she gets lots of email. You can send her more by addressing it to slee@cpg.com.